The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:
06/26/2013

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird applications, which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client.

Successful exploitation of these vulnerabilities could result in either an attacker can exploit these issues to execute arbitrary code in the context of the vulnerable application, crash affected applications, obtain potentially sensitive information, gain escalated privileges, bypass security restrictions, and perform unauthorized actions.

SYSTEMS AFFECTED:
- Firefox versions prior to 22.0
- Firefox Extended Support Release (ESR) versions prior to 17.0.7
- Thunderbird versions prior to 17.0.7
- Thunderbird Extended Support Release (ESR) versions prior to 17.0.7

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird. The details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2013-49) (CVE-2013-1682) (CVE-2013-1683): Multiple memory-corruption vulnerabilities exist in the browser engine that could lead to arbitrary code execution.

Memory corruption found using Address Sanitizer (MFSA 2013-50) (CVE-2013-1684) (CVE-2013-1685) (CVE-2013-1686): The Address Sanitizer tool can be used to trigger use-after-free, out of bounds read, and invalid write vulnerabilities. These issues are potentially exploitable and could lead to remote code execution.

Privileged content access and execution via XBL (MFSA 2013-51) (CVE-2013-1687): An attack can compile a user-defined function in the XBL scope of a specific element and then trigger the event to execute code.

Arbitrary code execution within Profiler (MFSA 2013-52) (CVE-2013-1688): Arbitrary code execution can occur when a user examines the profiler output on a malicious website containing specially crafted code.

Execution of unmapped memory through onreadystatechange event (MFSA 2013-53) (CVE-2013-1690): Specially crafted web content using the onreadystatechange event and reloading of pages could sometimes cause a crash when unmapped memory is executed.

Data in the body of XHR HEAD requests leads to CSRF attacks (MFSA 2013-54) (CVE-2013-1692): Firefox is sending data in the body of XMLHttpRequest (XHR) HEAD requests, which goes against the XHR specification. This can potentially be used for Cross-Site Request Forgery (CSRF) attacks against sites which do not distinguish between HEAD and POST requests.

SVG filters can lead to information disclosure (MFSA 2013-55) (CVE-2013-1693): Timing differences in the processing of SVG format images with filters could allow for pixel values to be read. This could potentially allow for text values to be read across domains, leading to information disclosure.

PreserveWrapper has inconsistent behavior (MFSA 2013-56) (CVE-2013-1694): PreserveWrapper can be used in cases where a wrapper is not set; the preserved-wrapper flag on the wrapper cache is cleared. This could potentially lead to an exploitable crash.

Sandbox restrictions not applied to nested frame elements (MFSA 2013-57) (CVE-2013-1695): <iframe sandbox> restrictions are not applied to aframe element contained within a sandboxed iframe. As a result, content hosted within a sandboxed iframe could use a frame element to bypass the restrictions that should be applied.

X-Frame-Options ignored when using server push with multi-part responses (MFSA 2013-58) (CVE-2013-1696): Firefox ignores the header for X-Frame-Options when the server uses push in multi-part responses. This can result in clickjacking on sites that use X-Frame-Options as a clickjacking protection.

XrayWrappers can be bypassed to run user defined methods in a privileged context (MFSA 2013-59) (CVE-2013-1697): XrayWrappers can be bypassed allowing attackers to use DefaultValue to call content-defined toString and valueof methods. This leads to un expected behavior when privileged code runs.

getUserMedia permission dialog incorrectly displays location (MFSA 2013-60) (CVE-2013-1698): WebPages imbedded in an iframe that call the getUserMedia permission dialog will display the origin as the top-level document. This can lead to users incorrectly giving permissions to malicious sites.

Homograph Domain spoofing in .com, .net and .name (MFSA 2013-61) (CVE-2013-1699): .com, .net, and .name where previously included on the Firefox Internationalized Domain Name (IDN) list. This could allow attackers to trick users into navigating to malicious domains.

Local privilege escalation through Mozilla Maintenance Service (MFSA 2013-62) (CVE-2013-1700): This vulnerability allows local unprivileged users to escalate their privileges through the system privileges used by the Mozilla Maintenance Service. Local file system access is necessary for this vulnerability to be exploited.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2013/mfsa2013-49.html
http://www.mozilla.org/security/announce/2013/mfsa2013-50.html
http://www.mozilla.org/security/announce/2013/mfsa2013-51.html
http://www.mozilla.org/security/announce/2013/mfsa2013-52.html
http://www.mozilla.org/security/announce/2013/mfsa2013-53.html
http://www.mozilla.org/security/announce/2013/mfsa2013-54.html
http://www.mozilla.org/security/announce/2013/mfsa2013-55.html
http://www.mozilla.org/security/announce/2013/mfsa2013-56.html
http://www.mozilla.org/security/announce/2013/mfsa2013-57.html
http://www.mozilla.org/security/announce/2013/mfsa2013-58.html
http://www.mozilla.org/security/announce/2013/mfsa2013-59.html
http://www.mozilla.org/security/announce/2013/mfsa2013-60.html
http://www.mozilla.org/security/announce/2013/mfsa2013-61.html
http://www.mozilla.org/security/announce/2013/mfsa2013-62.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1682
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1683
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1684
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1685
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1687
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1688
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1690
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1693
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1694
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1695
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1696
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1697
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1698
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1699

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1700